Manage End Users

Manage End Users Overview

For information about assigning users to IM and Presence Service nodes and to set up users for IM and Presence Service, see the following guides:

As part of your administrative tasks for managing end users, you may have to manage the following tasks:

- Configure a default policy for authorizing presence requests
- Configure a scheduled system check for duplicate or invalid user IDs and directory URIs
- Fix user ID and directory URI issues as they arise

For information on how to import and set up end users, see the "Configure End Users" section of the *System Configuration Guide for Cisco Unified Communications Manager*.

For information on completing bulk user contact list imports and exports, see Bulk Administration of Contact Lists.

Presence Authorization Overview

You must assign a system authorization policy for Presence Subscription requests. The Presence Authorization Policy determines, at a system level, whether end users on the system can view other end users' presence status without requiring the authorization of the end user whose presence is requested. This setting is configured via the **Allow users to view the availability of other users without being prompted for approval** check box in the **Presence Settings** configuration window. the available settings depends partially on which protocol is being deployed:

- For SIP-based clients, you must configure the IM and Presence Service to authorize automatically all presence subscription requests or Presence will not function correctly (this is the default setting). When this option is configured, the IM and Presence Service authorizes all requests automatically with one exception: if the user whose presence is being requested has a blocked list configured in their Cisco Jabber client that includes the user making the request. In this case, the user will be prompted to approve the Presence request.

- For XMPP-based clients, you can configure whether or not you want the IM and Presence Service to prompt users to authorize presence requests from other users, or whether those presence requests should be authorized automatically.

Note The authorization system settings can be overridden by the User Policy configuration that end users can configure within their Cisco Jabber clients

User Policy Settings in Jabber

When authorizing a presence request, the IM and Presence Service also refers to the user policy that users configure within their Cisco Jabber clients. End users can add other users to a blocked list, which prevents those other users from viewing presence status without authorization, or they can add those users to an allowed list, which authorizes those users to view their presence status. These settings override the system default settings:

End users can configure the following within their Cisco Jabber clients:

- Blocked list— Users can add other users (both local and external users) to a blocked list. If any users of the blocked users view that user's presence, they will always see the availability status of the user as unavailable regardless of the true status of the user. Users can also block a whole federated domain.
- Allowed list— Users can allow other local and external users to always be able to view their availability. The user can also allow a whole external (federated) domain.
- Default policy—The default policy settings for that user. The user can set the policy to block all users, or allow all users.

Validating User IDs and Directory URIs

For single cluster deployments, duplicate user IDs and directory URIs are not an issue as it is not possible to assign duplicates within the same cluster. However, with intercluster deployments, you can unintentionally assign the same user ID or directory URI value to different users on different clusters.

The IM and Presence Service provides the following validation tools to check for duplicate user IDs and duplicate directory URIs:

- Cisco IM and Presence Data Monitor service—You can configure ongoing system checks with this service. The Cisco IM and Presence Data Monitor service checks the active directory entries for duplicate user IDs and duplicate, or empty, directory URIs for all IM and Presence Service intercluster nodes. Administrators are notified via an alarm or alert. You can use the Cisco Unified Real-Time Monitoring Tool to monitor alarms and to set up email alerts for Duplicate UserID and DuplicateDirectoryURI errors..
- System Troubleshooter—Use the System Troubleshooter if you want to run an ad hoc check the system for errors, including duplicate directory URIs and user IDs. The Troubleshooter provides details for up to 10 users only. The System Troubleshooter can be accessed from the Cisco Unified CM IM and Presence Administration interface (**Diagnostics** > **System Troubleshooter**).
- Command Line Interface—To obtain a complete and detailed report of duplicate URIs and User IDs, run the `utils users validate all` CLI command.

Manage End Users Task Flow

Procedure

	Command or Action	Purpose
Step 1	Assign a Presence Authorization Policy, on page 3	Assign a system authorization policy for Presence Subscription requests.
Step 2	Configure Data Monitor Checks for User Data, on page 4	Configure the Cisco IM and Presence Data Monitor service to run scheduled checks for duplicate directory URIs and user IDs. A system alarm or alert is raised when an issue is found.
Step 3	Validate User Data via the System Troubleshooter, on page 6	Run the system troubleshooter if you want to run an ad hoc check for system issues, including duplicate directory URIs and user IDs.
Step 4	Validate User IDs and Directory URIs via CLI, on page 7	Run a CLI command to get a detailed report of duplicate directory URIs and user IDs.
Step 5	View Presence Settings for User, on page 10	If you want to view presence settings for an IM and Presence-enabled end user, you can use the Presence Viewer to view those settings.

Assign a Presence Authorization Policy

Assign a system authorization policy for Presence Subscription requests.

Note On their Cisco Jabber client, end users can configure whether they want to allow other users to be able to view their presence status. This user policy overrides the system authorization settings.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Presence** > **Settings**.

Step 2 Check or uncheck the **Allow users to view the availability of other users without being prompted for approval** check box.

- Checked—IM and Presence automatically authorizes all Presence subscription requests received within the local enterprise.
- Unchecked—IM and Presence refers all presence subscription requests to the client whose presence is requested. The user can accept or reject the request.

Note If you are deploying SIP-based clients, you must check this check box.If leave the check box unchecked, your deployment supports XMPP clients only.

Step 3 Click **Save**.

Step 4 Restart the Cisco XCP Router service.

What to do next

Proceed to configure the SIP publish trunk on IM and Presence Service.

Configure Data Monitor Checks for User Data

Complete these tasks to configure the Cisco IM and Presence Data Monitor to validate directory URIs and user IDs at scheduled intervals. Any errors are communicated via an alarm or alert with the Cisco Unified Real-Time Monitoring Tool.

Note Duplicate directory URI and duplicate user ID errors are only an issue for intercluster deployments.

Procedure

	Command or Action	Purpose
Step 1	Set Schedule for User ID and Directory URI Validation Check, on page 4	Configure the scheduled interval for the Cisco IM and Presence Data Monitor check. The service checks the active directory entries for errors, including duplicate directory URIs and user IDs.
Step 2	Set up Email Server for Email Alerts, on page 5	Optional. If you want to receive email alerts whenever the Data Monitor service finds a duplicate directory URI or user ID, you must set up an email server with the Real-Time Monitoring Tool.
Step 3	Enable Email Alerts, on page 5	Optional. Complete this procedure to enable email alerts for the DuplicateDirectoryURI and DuplicateUserid alarm. When the Cisco IM and Presence Data Monitor service returns one of these alarms, an email will be sent to the administrator.

Set Schedule for User ID and Directory URI Validation Check

Set the scheduled interval for the Cisco IM and Presence Data Monitor service. This service checks the system at scheduled intervals for data errors, including duplicate directory URIs and user IDs. The service raises an alarm or alert that can be viewed via the Real-Time Monitoring Tool whenever an error is found.

Before you begin

The Cisco IM and Presence Data Monitor network service must be running. By default, the service is running. You can confirm that the service is running from the **Control Center - Network Services** window in the Cisco Unified IM and Presence Serviceability interface.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters.**.

Step 2 In the **Service** drop-down, choose **Cisco IM and Presence Data Monitor**.

Step 3 In the **User Check Interval** field, enter the time interval, in minutes. You can enter an integer from 5 through 1440 (minutes). The default value is 30 minutes.

Step 4 Click **Save**.

What to do next

Optional. If you want to set up email alerting whenever a DuplicateDirectoryURI or DuplicateUserid alarm is raised, Set up Email Server for Email Alerts, on page 5

Set up Email Server for Email Alerts

It may help to have an administrator receive an email alert whenever the Data Monitor validation check finds duplicate directory URI and user ID errors. If so, use this optional procedure to set up an email server for email alerts.

Procedure

Step 1 In the Real-Time Monitoring Tool's System window, click **Alert Central**.

Step 2 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

Step 3 In the **Mail Server Configuration** popup, enter the details for the mail server.

Step 4 Click **OK**.

What to do next

Enable Email Alerts, on page 5

Enable Email Alerts

Use this procedure to set up the Real-Time Monitoring Tool to email an administrator whenever a DuplicateUserID or DuplicateDirectoryURI system alert is raised.

Before you begin

Set up Email Server for Email Alerts, on page 5

Procedure

Step 1 In the Real-Time Monitoring Tool **System** area, click **Alert Central**.

Step 2 Click the **IM and Presence** tab.

Step 3 Click on the alert for which you want to add an email alert. For example, the **DuplicateDirecytoryURI** or **DuplicateUserid** system alerts.

Step 4 Choose **Tools** > **Alert** > **Config Alert Action**.

Step 5 In the **Alert Action** popup, select **Default** and click **Edit**.

Step 6 In the **Alert Action** popup, **Add** a recipient.

Step 7 In the popup window, enter the address where you want to send email alerts, and click **OK** .

Step 8 In the **Alert Action** popup, make sure that the address appears under **Recipients** and that the **Enable** check box is checked.

Step 9 Click **OK**.

Step 10 Repeat this procedure for each system alert for which you want to enable email alerting.

Validate User Data via the System Troubleshooter

Use the System Troubleshooter in the Cisco Unified CM IM and Presence Administration GUI to check your deployment for duplicate user IDs and duplicate or invalid directory URIs. The troubleshooter checks all nodes and clusters in the deployment.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Diagnostics** > **System Troubleshooter**.

Step 2 Monitor the status of user IDs and Directory URIs in the **User Troubleshooter** area. The **Problem** column is populated if the system check detects any issues.

- Verify that all users have a unique User ID configured.
- Verify that all users have a Directory URI configured.
- Verify that all users have a unique Directory URI configured.
- Verify that all users have a valid Directory URI configured.
- Verify that all users have a unique Mail ID configured.

Note Duplicate mail IDs impact both Email Address for Federation and Exchange Calendar integration features.

Step 3 If an issue appears, click the **fix** link in the **Solution** column to be redirected to the **End User Configuration** window in Cisco Unified Communications Manager where you can reconfigure user settings.

Note The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

What to do next

If any issues arise, edit the user settings in the **End User Configuration** window of Cisco Unified Communications Manager. If the user is synchronized from an LDAP directory, you will need to make your edits in the LDAP directory.

If you need a more detailed report, Validate User IDs and Directory URIs via CLI, on page 7.

Validate User IDs and Directory URIs via CLI

Use the Command Line Interface to run a detailed check of your deployment for duplicate user IDs and duplicate directory URIs.

Procedure

Step 1 Login to the Command Line Interface.

Step 2 Run one of the following commands:.

- `utils users validate all`— Checks the system for both duplicate user IDs and duplicate directory URIs.
- `utils users validate userid`— Checks the system for duplicate user IDs.
- `utils users validate uri`— Checks the system for duplicate directory URIs.

The CLI returns a report of duplicate directory URIs and/or user IDs. For a sample report, see User ID and Directory URI CLI Validation Examples, on page 7

What to do next

If any issues arise, edit the user settings in the End User Configuration window of Cisco Unified Communications Manager. If the user is synchronized from an LDAP directory, you will need to make your edits in the LDAP directory.

User ID and Directory URI CLI Validation Examples

The CLI command to validate IM and Presence Service users to identify users that have duplicate user IDs and duplicate or invalid Directory URIs is utils users validate { all | userid | uri }.

The Directory URI must be unique for each user. You cannot use the same Directory URI for multiple users, irrespective of it being case-sensitive. For example, you cannot have two different Directory URI such as `aaa@bbb.ccc` and `AAA@BBB.CCC`, though they are case-sensitive.

For more information about using the CLI and command descriptions, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

CLI Example Output Showing User ID Errors

```
Users with Duplicate User IDs
---------------------------------------------
 User ID: user3
  Node Name
  cucm-imp-1
  cucm-imp-2
```

CLI Example Output Showing Directory URI Errors

```
Users with No Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
```

```
 User ID
 user4

Users with Invalid Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
-----------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

User ID and Directory URI Errors

The Cisco IM and Presence Data Monitor service checks the Active directory entries for duplicate user IDs and empty or duplicate directory URIs for all IM and Presence Service intercluster nodes. Duplicate user IDs or directory URIs are not possible within a cluster; however, it is possible to unintentionally assign the same user ID or directory URI value to users on different clusters in an intercluster deployment.

The following list displays possible errors that may be found. You can view these errors in the Real-Time Monitoring Tool, which will raise an alarm or alert for each of these:

DuplicateDirectoryURI

This alert indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the Directory URI IM Address scheme is configured.

DuplicateDirectoryURIWarning

This warning indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the `userID@Default_Domain` IM Address scheme is configured.

DuplicateUserid

This alert indicates there are duplicate user IDs assigned to one or more users on different clusters within the intercluster deployment.

InvalidDirectoryURI

This alert indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the Directory URI IM Address scheme is configured.

InvalidDirectoryURIWarning

This warning indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the `userID@Default_Domain` IM Address scheme is configured.

To gather specific information about which users have these alarm conditions, use the Command Line Interface for a complete listing. System alarms do not provide details about the affected users and the System Troubleshooter displays details for only up to 10 users. Use the Command Line Interface and validate users to gather information about which users caused an alarm. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Caution Take the appropriate action to fix duplicate user IDs and duplicate or invalid Directory URIs to avoid communications disruptions for the affected users. To modify user contact information, see the *Cisco Unified Communications Manager Administration Guide*.

Errors and Suggested Action

The following table describes user ID and directory URI error conditions that can occur when a system check for duplicate user IDs and duplicate or invalid directory URIs is performed on an intercluster deployment. The alarms that are raised are listed, as well as suggested actions to take to correct the error.

Table 1: User ID and Directory URI Error Conditions and Suggested Action

Error Condition	Description	Suggested Action
Duplicate user IDs	Duplicate user IDs are assigned to one or more users on different clusters within the intercluster deployment. The affected users may be homed on an intercluster peer. **Related alarms:** `DuplicateUserid`	If the `DuplicateUserid` alert is raised, take immediate action to correct the issue. Each user within the intercluster deployment must have a unique user ID.
Duplicate directory URIs	Multiple users within the intercluster deployment are assigned the same directory URI value. The affected users may be homed on an intercluster peer. **Related alarms:** • `DuplicateDirectoryURI` • `DuplicateDirectoryURIWarning`	If your system is configured to use the Directory URI IM address scheme and the `DuplicateDirectoryURI` alert is raised, take immediate action to correct the issue. Each user must be assigned a unique directory URI. If your system is configured to use the *userID@Default_Domain* IM address scheme and duplicate directory URIs are detected, the `DuplicateDirectoryURIWarning` warning is raised and no immediate action is required; however, Cisco recommends that you resolve the issue.

Error Condition	Description	Suggested Action
Invalid directory URIs	One or more users within the deployment are assigned an invalid or empty directory URI value. A URI that is not in the *user@domain* format is an invalid Directory URI. The affected users may be homed on an intercluster peer. **Related alarms:** • `InvalidDirectoryURI` • `InvalidDirectoryURIWarning`	If your system is configured to use the Directory URI IM address scheme and the following alert is raised, take immediate action to correct the issue:`InvalidDirectoryURI`. If your system is configured to use the *userID@Default_Domain* IM address scheme and invalid directory URIs are detected, the `InvalidDirectoryURIWarning` warning is raised and no immediate action is required; however, Cisco recommends that you resolve the issue.

View Presence Settings for User

Use the Presence Viewer to get a summarized view of presence settings for an IM and Presence-enabled end user. The Presence Viewer provides information such as Presence server assignments, contacts and watchers.

Before you begin

The **Cisco AXL Web Service**, **Cisco SIP Proxy** service, and **Cisco Presence Engine** service must all be running in Cisco Unified Serviceability.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End Users**.

Step 2 Click **Find** and select the end user for whom you want to view presence settings.

Step 3 Under **Service Settings**, click **Presence Viewer for User** to open the Presence Viewer. Refer to the following table if you want to customize the view.

Table 2: End User Presence Viewer Fields

Presence Setting	Description
User Status	Identifies the availability state of the user, including: • Available • Away • Do Not Disturb • Unavailable • Custom

Presence Setting	Description
User ID	Identifies the selected user ID. A user photo is displayed if one is available for that user. You can click **Submit** to choose a different User ID.
View From Perspective of	Specifies a user to see the availability status from the perspective of the user. This allows you to determine how the availability status of a specified user appears to another user, known as a watcher. This functionality is useful in debugging scenarios, for example, where a user has configured privacy policies. A maximum of 128 characters is allowed.
Contacts	Displays the number of contacts in the contact list for this user. Click the arrow beside the Contacts heading in the Contacts and Watchers list area to view the availability status of a specific user contact. Click the arrow beside the group name to expand the list of contacts within that group. Contacts that are not part of a group (groupless contacts) display below the contact group list. A contact may belong to multiple groups, but will only count once against the contact list size for that user. A warning message appears if the maximum number of contacts configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum contacts setting, see the *IM and Presence Administration Online Help*.
Watchers	Displays a list of users, known as watchers, who have subscribed to see the availability status of this user in their contact list. Click the arrow beside the Watchers heading in the Contacts and Watchers list area to view the availability status of a specific watcher. Click the arrow beside the group name to expand the list of watchers within that group. A watcher may belong to multiple groups but will only count once against the watcher list size for that user. A warning message appears if the maximum number of watchers configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum watchers setting, see the *IM and Presence Administration Online Help*.
Presence Server Assignment	Identifies the IM and Presence Service server to which the user is assigned. Hyperlinks allow you to go directly to the server configuration page for details.
Enable accessible presence icons	Select this check box to enable presence accessibility icons for this end user.
Submit	Select to run the Presence Viewer. The user must be assigned to an IM and Presence node for valid presence information to be available. The AXL, Presence Engine and Proxy Service must all be running on the IM and Presence server for this action to be functional.

Presence Authorization Interactions and Restrictions

Feature	Restriction
Turning off automatic presence authorization	If you turn off automatic authorization of presence requests, IM and Presence Service still automatically authorizes subscription requests for users that are on the contact list of the other user. This applies to users in the same domain, and users in different domains (federated users). For example: • User A wishes to subscribe the view the availability status of User B. Automatic authorization is off on IM and Presence Service, and User B is not in the Allowed or Blocked list for the User A • IM and Presence Service sends the presence subscription request to the client application of User B, and the client application prompts User B to accept or reject the subscription. • User B accepts the presence subscription request, and User B is added to the contact list of User A. • User A is then automatically added to the contact list for User B without being prompted to authorize the presence subscription. This occurs even if the policy for User B blocks the external domain, or User B has "ask me" configured in the user profile.
Interdomain Federation—Presence requests received from the external domain	IM and Presence will rely solely on the user policy settings of the user whose presence status is requested. If the user has selected "ask me" in their user policy, and has not added an Allowed or Blocked list for the external contact or domain, then IM and Presence sends the Presence request to the end user to authorize.